We Claim:

1. A method for authenticating a data set between a proving unit and a verifying unit, which comprises the steps of:

a) communicating the data set from one of the proving and verifying units to a respective other of the proving and verifying units such that the data set is in an unencrypted form to both the proving and verifying units after completing the communicating step;

b) generating at least one data element in the verifying unit;

c) using the verifying unit to encrypt the data element in a first cryptographic encryption method using a public key of the proving unit resulting in at least one encrypted data element, and the public key is known to the verifying unit;

d) communicating the encrypted data element from the verifying unit to the proving unit;

e) using the proving unit to decrypt the encrypted data element in a first decryption method, assigned to the first encryption method, using a private key known only to the proving unit;

f) using the proving unit to calculate, from the data set to be authenticated, in a second cryptographic method, an authenticator dependent on the data element;

g) communicating the authenticator from the proving unit to the verifying unit;

h) using the verifying unit to check the authenticator with an aid of an authentication checking algorithm, assigned to the second cryptographic method using the data element and the data set; and

i) accepting the data set as communicated by the proving unit to the verifying unit in dependence on a result of the checking step.

2. The method according to claim 1, which further comprises during the step a), using the proving unit to communicate the data set in unencrypted form to the verifying unit.

3. The method according to claim 1, which further comprises using the verifying unit to generate the data set as a random element and subsequently, in the step a), communicating the data set to the proving unit.

4. The method according to claim 1, which further comprises during the step h):

forming the authentication checking algorithm to be substantially identical to the second cryptographic method for authenticator generation;

applying the authentication checking algorithm by the verifying unit to the data element and the data set for forming a reference authenticator; and

comparing the reference authenticator with the authenticator.

5. The method according to claim 1, which further comprises during the step h):

forming the authentication checking algorithm with a decryption method corresponding to the second cryptographic method for generating the authenticator for an associated encryption method;

applying the authentication checking algorithm by the verifying unit to the authenticator by decryption for forming a reference data element and a reference data set; and

comparing the reference data element and the reference data set with the data element and the data set.

6. The method according to claim 1, which further comprises:

repeating steps b), c), d) and e) for generating at least one further data element before performing the step f); and

using the proving unit to encrypt the data set to be authenticated in step f) in a manner dependent on the data element and the further data element to form the authenticator.

7. The method according to claim 1, which further comprises carrying out the first cryptographic encryption method and the first decryption method assigned thereto using discrete exponentiation in a semigroup.

8. The method according to claim 7, which further comprises carrying out the first cryptographic encryption method and the first decryption method assigned thereto using an algorithm based on elliptical curves.

9. The method according to claim 7, which further comprises performing the first cryptographic encryption method with the steps of:

using the verifying unit to generate a number $t \in T$, where T is a subrange of integers;

using the verifying unit to calculate element $h^{f(t)} \in H$, where $f : T \rightarrow T'$ is a mapping into a subrange T' of the integers, which is not necessarily different from T, H represents a multiplicatively written semigroup generated by element h, with a discrete exponentiation of a base h as a one-way function in the semigroup H;

using the verifying unit to calculate from the public key, $k_{pub} = h^{f(d)} \in H$, element $\pi(k_{pub}{}^{f(t)}) \in G$, where $\pi : H \rightarrow G$ specifies a mapping of the semigroup H into a group G, $d \equiv k_{priv} \in T$ is the private key which is accessible only to the proving unit, and a mapping $t \rightarrow h^{f(t)} \rightarrow \pi(h^{f(t)})$ from the subrange of the integers T to the group G represents a one-way function; and

using the verifying unit to encrypt the data element, z, by a combination with respect to the encrypted data element, $z' = z \circ \pi(k_{pub}{}^{f(t)}) \in G$.

10. The method according to claim 9, which further comprises during the step d), in addition to the encrypted data element,

using the verifying unit to communicate the element $h^{f(t)} \in H$ to the proving unit.

11. The method according to claim 10, which further comprises performing the first cryptographic decryption method by the steps of:

using the proving unit to calculate the element $k_{pub}{}^{f(t)} \in H$ using function f, the element $h^{f(t)} \in H$ and the private key d known only to the proving unit;

using the proving unit to calculate an inverse element $\pi'(k_{pub}{}^{f(t)}) \in G$ with respect to element $\pi(k_{pub}{}^{f(t)}) \in G$; and

using the proving unit to decrypt the encrypted data element by a combination of the encrypted data element with inverse element: $z = z' \circ \pi'(k_{pub}{}^{f(t)})$, where the first cryptographic decryption method is based on the same mappings f, π and the same combination $\circ$ as the first cryptographic encryption method.

12. The method according to claim 11, which further comprises performing the second cryptographic method with the steps of:

using the proving unit to calculate, from the at least one unencrypted data element z, an element $g_2 = \pi_1(z) \in G_1$ and an element $g_2 = \pi_2(z) \in G_2$, where $G-_1$ and G_2 represent groups where $G_1 \subset G_2$ and $\pi_1 : G \rightarrow G_1$ and $\pi_2 : G \rightarrow G_2$ represent functions which map elements of the group G onto the groups G_1 or G_2;

using the proving unit to transform the data set to be authenticated m, to form an element $g' = (g_1 * m)$ with a group combination * in G_1; and

using the proving unit to calculate the authenticator D, by $D = inj(g') \bullet g_2$ with the group combination $\bullet$ in G_2, where the mapping $inj : G_1 \rightarrow G_2$ maps elements from G_1 injectively into G_2.

13. The method according to claim 1, which further comprises performing the following steps before performing step b):

using the proving unit to communicate the public key with a certificate of a trust center;

using the verifying unit to check a validity of the public key of the proving unit using a certification method; and

using the verifying unit to continue the communication with the proving unit in a manner dependent on a result of the check.

14. The method according to claim 1, which further comprises:

forming the proving unit as an integrated circuit on a smart card; and

forming the verifying unit as a smart card terminal.

15. The method according to claim 1, which further comprises forming the proving unit as an integrated circuit in an identification/authentication token which is fixedly connected to a non-localized object.

16. The method according to claim 14, which further comprises performing the communication between the proving unit and the verifying unit contactlessly.

17. The method according to claim 8, which further comprises performing the first cryptographic encryption method with the steps of:

using the verifying unit to generate a number $t \in T$, where T is a subrange of integers;

using the verifying unit to calculate element $h^{f(t)} \in H$, where $f : T \rightarrow T'$ is a mapping into a subrange T' of the integers, which is not necessarily different from T, H represents a multiplicatively written semigroup generated by element h, with a discrete exponentiation of a base h as one-way function in the semigroup H;

using the verifying unit to calculate from the public key, $k_{pub} = h^{f(d)} \in H$, element $\pi(k_{pub}{}^{f(t)}) \in G$, where $\pi : H \rightarrow G$ specifies a mapping of the semigroup H into a group G, $d \equiv k_{priv} \in T$ is the private key which is accessible only to the proving unit, and a mapping $t \rightarrow h^{f(t)} \rightarrow \pi(h^{f(t)})$ from the subrange of the integers T to the group G represents a one-way function; and

using the verifying unit to encrypt the at least one data element, z, by a combination with respect to the encrypted data element, $z' = z \circ \pi(k_{pub}{}^{f(t)}) \in G$.

18. The method according to claim 17, which further comprises during the step d), in addition to the encrypted data element, using the verifying unit to communicate the element $h^{f(t)} \in H$ to the proving unit.

19. The method according to claim 18, which further comprises performing the first cryptographic decryption method by the steps of:

using the proving unit to calculate the element $k_{pub}^{f(t)} \in H$ using function f, the element $h^{f(t)} \in H$ and the private key d known only to the proving unit;

using the proving unit to calculate an inverse element $\pi'(k_{pub}^{f(t)}) \in G$ with respect to element $\pi(k_{pub}^{f(t)}) \in G$; and

using the proving unit to decrypt the encrypted data element by a combination of the encrypted data element with inverse element: $z = z' \circ \pi'(k_{pub}^{f(t)})$, where the first cryptographic decryption method is based on the same mappings f, π and the same combination $\circ$ as the first cryptographic encryption method.

20. The method according to claim 19, which further comprises performing the second cryptographic method with the steps of:

using the proving unit to calculate, from the at least one unencrypted data element z, an element $g_2 = \pi_1(z) \in G_1$ and an element $g_2 = \pi_2(z) \in G_2$, where $G-_1$ and G_2 represent groups where

$G_1 \subset G_2$ and $\pi_1 : G \rightarrow G_1$ and $\pi_2 : G \rightarrow G_2$ represent functions which map elements of the group G onto the groups G_1 or G_2;

using the proving unit to transform the data set to be authenticated m, to form an element $g' = (g_1 * m)$ with a group combination $*$ in G_1; and

using the proving unit to calculate the authenticator D, by $D = inj(g') \bullet g_2$ with the group combination $\bullet$ in G_2, where the mapping $inj : G_1 \rightarrow G_2$ maps elements from G_1 injectively into G_2.

21. The method according to claim 15, which further comprises performing the communication between the proving unit and the verifying unit contactlessly.